

WHAT IS CLAIMED IS:

1. A reconfigurable secure keyboard console to encrypt a keystroke, comprising:
 - a plurality of physical keys;
 - a reconfigurable first memory to an encryption key;
 - a reconfigurable second memory to store at least one transformation instruction;
 - a reconfigurable third memory; and
 - a keyboard processor including a standard lookup table containing a plurality of codes and a plurality of values, each of the plurality of codes and the plurality of values corresponding to one of a plurality of potential keyboard inputs,

wherein the keyboard processor retrieves the at least one transformation instruction,

executes the at least one transformation instruction,

creates a transformed lookup table containing the plurality of values and a plurality of transformed codes, each of the plurality of values and the plurality of transformed codes corresponding to one of the plurality of potential keyboard inputs,

stores the transformed lookup table in the third reconfigurable memory,

receives actual keyboard input corresponding to one of the plurality of potential keyboard inputs and finds an actual value corresponding to one of the plurality of potential keyboard inputs;

matches the actual value with one of the plurality of values in the transformed lookup table; and

outputs a transformed code from the plurality of transformed codes corresponding to the actual value.

- 20190723 100827.000
2. The reconfigurable secure keyboard console of claim 1, wherein the first reconfigurable memory and the second reconfigurable memory are both located in the same physical memory device.
 3. The reconfigurable secure keyboard console of claim 1, wherein the first reconfigurable memory, the second reconfigurable memory and the third reconfigurable memory are located in the same physical memory device.
 4. The reconfigurable secure keyboard console of claim 1, further including a transaction card reader.
 5. The reconfigurable secure keyboard console of claim 4, wherein the transaction card reader is a smart card reader.
 6. The reconfigurable secure keyboard console of claim 5, wherein a subscriber identity module (SIM) is plugged into the smart card reader
 7. The reconfigurable secure keyboard console of claim 4, wherein the transaction card reader is a bar code reader.
 8. The reconfigurable secure keyboard console of claim 4, wherein the transaction card reader is a biometric reader.
 9. The reconfigurable secure keyboard console of claim 4, wherein the transaction card reader is a memory card reader.
 10. A computing device, comprising:
 - a central processing unit (CPU);
 - a keyboard controller to receive encrypted data from the reconfigurable secure keyboard console; and

a reconfigurable secure keyboard console to transmit encrypted data to the keyboard controller including,

- a plurality of physical keys,

- a reconfigurable first memory to an encryption key,

- a reconfigurable second memory to store at least one transformation instruction,

- a reconfigurable third memory, and

- a keyboard processor including a standard lookup table containing a plurality of codes and a plurality of values, each of the plurality of codes and the plurality of values corresponding to one of a plurality of potential keyboard inputs,

- wherein the keyboard processor retrieves the at least one transformation instruction,

- executes the at least one transformation instruction,

- creates a transformed lookup table containing the plurality of values and a plurality of transformed codes, each of the plurality of values and the plurality of transformed codes corresponding to one of the plurality of potential keyboard inputs,

- stores the transformed lookup table in the third reconfigurable memory,

- receives actual keyboard input corresponding to one of the plurality of potential keyboard inputs and finds an actual value corresponding to one of the plurality of potential keyboard inputs,

- matches the actual value with one of the plurality of values in the transformed lookup table, and

- outputs a transformed code from the plurality of transformed codes corresponding to the actual value.

11. A secure computing system, comprising:

a global network;

a first computing device to communicate securely with a second computing device over the global network, including

a first central processing unit to receive encrypted information from the global network and to transmit encrypted information to the global network,

a reconfigurable secure keyboard console to transmit encrypted information and to receive encrypted information from the keyboard controller including

a plurality of physical keys,

a reconfigurable first memory to an encryption key,

a reconfigurable second memory to store at least one transformation instruction,

a reconfigurable third memory, and

a keyboard processor including a standard lookup table containing a plurality of codes and a plurality of values, each of the plurality of codes and the plurality of values corresponding to one of a plurality of potential keyboard inputs,

wherein the keyboard processor retrieves the at least one transformation instruction,

executes the at least one transformation instruction,

creates a transformed lookup table containing the plurality of values and a plurality of transformed codes, each of the plurality of values and the plurality of transformed codes corresponding to one of the plurality of potential keyboard inputs,

stores the transformed lookup table in the third reconfigurable memory,

receives actual keyboard input corresponding to one of the plurality of potential keyboard inputs and finds an actual value corresponding to one of the plurality of potential keyboard inputs,

matches the actual value with one of the plurality of values in the transformed lookup table, and

outputs a transformed code from the plurality of transformed codes corresponding to the actual value, and

a keyboard controller to receive encrypted information from the secure keyboard console and to output encrypted information to the first central processing unit, and the second computing device communicates securely with the first computing device and includes

a central processing unit to receive encrypted information from the global network, transmit encrypted information to the global network, generate at least one transformation instruction, and

an encryption engine to generate encrypted information.

12. A method of encrypting keyboard input of a reconfigurable secure keyboard console, comprising:
 - receiving an encryption key and at least one transformation instruction from a computing device;
 - storing the encryption key in a reconfigurable first memory;
 - storing the at least one transformation instruction in a reconfigurable second memory;

utilizing the at least one transformation instruction to create a plurality of transformed codes, each of the plurality of encrypted transformed corresponding to one of a plurality of potential keyboard inputs from the reconfigurable secure keyboard console;

storing the plurality of transformed codes along with a plurality of values in a transformed lookup table, wherein the plurality of values corresponds to each of the plurality of potential keyboard inputs;

receiving an actual keyboard input;

matching the actual keyboard input with one of the plurality of the potential keyboard inputs to create a matching value; and

outputting a transformed code from the transformed lookup table corresponding to the matching value.

13. A program code storage device, comprising:

a machine-readable storage medium; and

machine-readable program code, stored on the machine-readable storage medium, the machine-readable program code having instructions to

receive an encryption key and at least one transformation from a computing device;

store the encryption key in a first reconfigurable memory;

store the at least one transformation instruction in a reconfigurable second memory;

utilize the at least one transformation instruction to create a plurality of transformed codes, each of the plurality of encrypted transformed corresponding to one of a plurality of potential keyboard inputs from a reconfigurable secure keyboard console;

store the plurality of transformed codes along with a plurality of values in a transformed lookup table, wherein the plurality of values corresponds to each of the plurality of potential keyboard inputs;

receive an actual keyboard input;

match the actual keyboard input with one of the plurality of the values which correspond to each of the potential keyboard inputs to create a matching value; and

output a transformed code from the transformed lookup table corresponding to the matching value.

2016-09-29 10:29:00